

Claims

1. A data processing system comprising a recorder/reproducer and a recording device for executing transmission of encryption data to each other, characterized in that:

said recording device has a data storing section for storing content data that is transferable between the recorder/reproducer and the recording device, and at the same time, has a plurality of key blocks storing key data applicable at least to authentication processing between the recorder/reproducer and the recording device, and the key data stored in the plurality of key blocks has a configuration in which different key data is stored for each block;

said recorder/reproducer has a configuration for, in the authentication processing between the recorder/reproducer and the recording device, designating one key block out of the plurality of key blocks held by said recording device, and executing the authentication processing with said recording device based on the key data stored in the designated key block.

2. The data processing system according to Claim 1, characterized in that an authentication key that is applicable at least to the authentication processing is included in each of the plurality of key blocks of said recording device, and the authentication key of each key block is configured as key data different from each other.

3. The data processing system according to Claim 1,
characterized by having a configuration in which:

said recorder/reproducer holds setting information in which a
key block to be applied to the authentication processing as a
designated key block in a memory in the recorder/reproducer; and

said recorder/reproducer designates one key block out of the
plurality of key blocks held by said recording device based on the
setting information held in the memory in the recorder/reproducer
when the authentication processing between the recorder/reproducer
and the recording device is performed, and executes the
authentication processing.

4. The data processing system according to Claim 3,
characterized by having a configuration in which the designated
key block setting information of said recorder/reproducer is set
to be different for each predetermined product unit such as a
model of the recorder/reproducer, a version or a delivery
destination.

5. The data processing system according to Claim 1,
characterized in that:

said recorder/reproducer has a configuration in which
authentication processing key data required for the authentication

processing with said recording device is stored in the memory in the recorder/reproducer; and

authentication of the authentication processing key data stored in said memory in the recorder/reproducer is only established in the authentication processing using a key data in a block stored in a part of the plurality of key blocks in said recording device, and is not established in the authentication processing using a key data in other key blocks.

6. The data processing system according to Claim 1, characterized in that:

said recorder/reproducer stores a master key M_{ake} for recording device authentication key in the memory of the recorder/reproducer; and

an authentication key K_{ake} that is generated based on said master key M_{ake} for recording device authentication key is an authentication key whose authentication is only established in the authentication processing using key data in a designated block set in the recorder/reproducer, and is not established in the authentication processing using key data in other key blocks.

7. The data processing system according to Claim 6, characterized in that:

said recording device has a configuration in which a recording device identification information ID_{mem} in said memory

in the recording device and, at the same time, an authentication key Kake that is different for each key block is stored in each of said plurality of key blocks; and

said recorder/reproducer has a configuration for generating the authentication key Kake by encryption processing of said recording device identification information IDmem based on the master key Mlake for recording device authentication stored in the memory of the recorder/reproducer, and performing the authentication processing with the designated key block of said recording device using the generated authentication key Kake.

8. The data processing system according to Claim 1, characterized in that each key block of said recording device includes recording device identifier information that is peculiar information of the recording device, an authentication key and a random number generation key to be used in the authentication processing with the recorder/reproducer, and a storing key to be used in encryption processing of storage data in said data storage section.

9. The data processing system according to Claim 8, characterized in that:

said storing key stored in each of the plurality of key blocks of said recording device is key data that is different for each key block and, at the same time, is a key to be used in

encryption processing with respect to stored data of said data storage section; and

said recording device has a configuration for executing key exchange processing of the storing key in the recording device, and outputting encryption data by a key different from the storing key to outside the recording device if utilization request of data that is encrypted by the storing key received from outside the recording device.

10. The data processing system according to Claim 1, characterized in that:

said recording device has an encryption processing section; and

the encryption processing section has a configuration for selecting one key block of the plurality of key blocks of the recording device in accordance with the key block designation information received from said recorder/reproducer, and executing the authentication processing with said recorder/reproducer using the key data in the selected key block.

11. The data processing system according to Claim 10, characterized in that the encryption processing section of said recording device has a configuration for executing the encryption processing executed in the data storing processing in the data storing section storing content data transferable between the

recorder/reproducer and the recording device and in the data transfer processing from the data storing section, using the key data in one key block that is selected in accordance with the key block designation information received from said recorder/reproducer.

12. The data processing system according to Claim 1, characterized in that there are a plurality of designatable key blocks in said recording device in said recorder/reproducer, and at least one key block in the plurality of designatable key blocks is configured as a commonly designatable key block that is also designatable in other recorder/reproducers.

13. A recording device having a data storage section for storing content data transferable with an external apparatus, characterized by having a plurality of key blocks storing key data applicable at least to authentication processing between the recording device and said external device, and key data stored the plurality of key blocks has a configuration for storing key data for each block.

14. The recording device according to Claim 13, characterized in that each of the plurality of key blocks of said recording device includes an authentication key applicable at least to the

authentication processing, and an authentication key for each key block is configured as key data that is different from each other.

15. The recording device according to Claim 13, characterized in that said recording device has a configuration in which a memory in said recording device has recording device identification information IDmem and, at the same time, a different authentication key Kake for each key block is stored in each of the plurality of key blocks.

16. The recording device according to Claim 13, characterized in that each key block of said recording device includes recording device identifier information that is peculiar information of the recording device, an authentication key and a random number generation key to be used in the authentication processing with said external apparatus, and a storing key to be used in encryption processing of storage data in said data storage section.

17. The recording device according to Claim 16, characterized in that:

said storing stored in each of the plurality of key blocks of said recording device is key data that is different for each key block and, at the same time, is a key to be used in encryption processing with respect to stored data of said data storage section; and

said recording device has a configuration for executing key exchange processing of the storing key in the recording device, and outputting encryption data by a key different from the storing key to outside the recording device if utilization request of data that is encrypted by the storing key is received from outside the recording device.

18. The recording device according to Claim 13, characterized in that:

said recording device has an encryption processing section;
and

the encryption processing section has a configuration for selecting on key block of the plurality of key blocks of the recording device in accordance with the key block designation information received from said external apparatus, and executing the authentication processing with said recorder/reproducer using the key data in the selected key block.

19. The recording device according to Claim 18, characterized in that the encryption processing section of said recording device has a configuration for executing the encryption processing executed in the data storing processing in the data storing section storing content data transferable between said external apparatus and the recording device and in the data transfer processing from the data storing section, using the key data in

one key block that is selected in accordance with the key block designation information received from said external apparatus.

20. A data processing method in a data processing system comprising a recorder/reproducer and a recording device for executing transmission of encryption data to each other, characterized in that a recorder/reproducer designates one key block out of a plurality of key blocks held by the recording device, and executes authentication processing with said recording device based on key data stored in the designated key block.

21. The data processing method according to Claim 20 characterized in that an authentication key that is applicable at least to the authentication processing is included in each of the plurality of key blocks of said recording device, and the authentication key of each key block is configured as key data different from each other.

22. The data processing method according to Claim 20 characterized in that said recorder/reproducer designates one key block out of the plurality of key blocks held by said recording device based on the setting information held in the memory in the recorder/reproducer when the authentication processing between the recorder/reproducer and the recording device is performed, and executes the authentication processing.

23. The data processing method according to Claim 20 characterized in that said recorder/reproducer stores a master key M_{ake} for recording device authentication key in the memory of the recorder/reproducer, generates an authentication key K_{ake} based on said master key M_{ake} for recording device authentication key, and executes authentication processing using key data in the designated key block of the plurality of key blocks held by said recording device using the generated authentication key K_{ake}.

24. The data processing method according to Claim 20 characterized in that:

said recording device has a configuration in which a recording device identification information ID_{mem} in said memory in the recording device and, at the same time, an authentication key K_{ake} that is different for each key block is stored in each of said plurality of key blocks; and

said recorder/reproducer generates the authentication key K_{ake} by executing encryption processing of said recording device identification information ID_{mem} based on the master key M_{ake} for recording device authentication stored in the memory of the recorder/reproducer, and performing the authentication processing with the designated key block of said recording device using the generated authentication key K_{ake}.

25. The data processing method according to Claim 20 characterized in that said recording device selects one key block of the plurality of key blocks of the recording device in accordance with the key block designation information received from said recorder/reproducer, and executes the authentication processing with said recorder/reproducer using the key data in the selected key block.

26. The data processing method according to Claim 20 characterized in that said recording device executes the encryption processing executed in the data storing processing in the data storing section storing content data transferable between the recorder/reproducer and the recording device and in the data transfer processing from the data storing section, using the key data in one key block that is selected in accordance with the key block designation information received from said recorder/reproducer.

27. The data processing method according to Claim 20 characterized in that:

each of the plurality of key blocks of said recording device includes a storing key used in encryption processing of stored data of the data storage section in said recording device; and

00037500-500450

said recording device executes key exchange processing of the storing key in the recording device, and outputting encryption data by a key different from the storing key to outside the recording device if utilization request of data that is encrypted by the storing key received from outside the recording device.

28. A program providing medium for providing a computer program that causes a computer system to execute a data processing method in a data processing system comprising a recorder/reproducer and a recording device for executing transmission of encryption data to each other, characterized in that said computer program includes a step in which a recorder/reproducer designates one key block out of a plurality of key blocks held by the recording device, and executes authentication processing with said recording device based on key data stored in the designated key block.

29. A data processing system comprising a first apparatus and a second apparatus for executing transmission of encryption data to each other, characterized in that:

said second apparatus has an encryption processing section for executing encryption processing for transmission data with said first apparatus;

said encryption processing section has a control section for receiving a command identifier transferred from said first apparatus in accordance with a setting sequence defined in advance,

taking out a command corresponding to the received command identifier from a register, and having the command executed; and

the control section has a configuration for, if the command identifier transferred from the first apparatus is a command identifier different from the setting sequence, canceling processing of command corresponding to the command identifier.

30. The data processing system according to Claim 29, characterized by having a configuration in which:

the setting sequence relating to the command identifier received from the first apparatus held by the control section is a command number setting sequence in which numbers are sequentially incremented; and

said control section stores a received value of the command number received from said first apparatus in a memory, determines coincidence of a new command number received from said first apparatus with the setting sequence based on the received command number stored in said memory and, if it is determined that the new received command number is different from the setting sequence, executes resetting of the command number stored in said memory without performing command processing corresponding to the new received command number.

31. The data processing system according to Claim 29, characterized in that:

said second apparatus has a command register storing a command in accordance with said setting sequence;

an authentication processing command sequence for executing authentication processing between said first apparatus and said second apparatus, and an encryption processing command sequence for executing encryption processing relating to transferred data between said first apparatus and said second apparatus; and

a sequence is set such that a command identifier corresponding to said authentication processing command sequence is executed in a step before a command sequence corresponding to said encryption processing command sequence.

32. The data processing system according to Claim 31, characterized in that said encryption processing command sequence includes at least one of a command sequence including encryption key exchange processing for encryption data that is transferred from said first apparatus to said second apparatus and stored in storing means in said second apparatus, or a command sequence including an encryption key exchange processing for encryption data that is stored in the storing means in said second apparatus and transferred from said second apparatus to said first apparatus.

33. The data processing system according to Claim 31, characterized in that said control section set an authentication flag indicating that authentication is done if authentication is

established by the authentication processing of said first apparatus and said second apparatus, and executes command management control that enables execution of said encryption processing command sequence during the authentication flag is set, and said control section resets said authentication flag in executing said authentication processing command sequence anew.

34. The data processing system according to Claim 32, characterized in that said data processing system has a configuration in which said control section manages an order of command execution based on said setting sequence and said command identifier in said encryption key exchange processing, and said control section does not accept command processing that is different from said setting sequence from an external apparatus including said first apparatus during a series of command execution relating to said key exchange processing.

35. The data processing system according to Claim 29, characterized in that:

said second apparatus is a storage device having a data storage section for storing encryption data;

said first apparatus is a recorder/reproducer for performing storing processing of data in said storage device, and taking out data stored in said storage device to reproduce and execute the data; and

said recorder/reproducer has an encryption processing section for executing encryption processing of transferred data with said recording device.

36. The data processing system according to Claim 35, characterized by having a configuration in which:

said recording device has a key block storing an authentication key applied to authentication processing between said recorder/reproducer and said recording device and a storing key as an encryption key of data stored in a data storage section in said recording device; and

said control section in an encryption processing section of said recording device receives a command identifier from said recorder/reproducer and executes authentication processing using the authentication key stored in said key block in accordance with said setting sequence, and executes encryption processing of data accompanying key exchange processing using said storing key after completing the authentication processing.

37. The data processing system according to Claim 36, characterized by having a configuration in which:

said key block is composed of a plurality of key blocks storing an authentication key and a storing key that are different each other; and

said recorder/reproducer notifies said recording device of one key block used in authentication processing and encryption processing of data as a designated key block out of said plurality of key blocks, and said recording device executes authentication processing using the authentication key stored in the designated key block and encryption processing of data using the storing key.

38. A recording device having a data storage section for storing content data that is transferable with an external apparatus, characterized in that:

said recording device has an encryption processing section for executing encryption processing for transmission data with an external apparatus;

said encryption processing section has a control section for receiving a command identifier transferred from said external apparatus in accordance with a setting sequence defined in advance, taking out a command corresponding to the received command

identifier from a register, and having the command executed; and

the control section has a configuration for, if the command identifier transferred from said external apparatus is a command identifier different from the setting sequence, canceling processing of command corresponding to the command identifier.

39. The recording device according to Claim 38, characterized in that:

00000000-00000000
said control section has a command number setting sequence in which numbers are sequentially incremented as said setting sequence; and

said control section has a configuration for storing a received value of the command number received from said external apparatus in a memory, determines coincidence of a new command number received from said external apparatus with the setting sequence based on the received command number stored in said memory and, if it is determined that the new received command number is different from the setting sequence, executes resetting of the command number stored in said memory without performing command processing corresponding to the new received command number.

40. The recording device according to Claim 38, characterized in that:

said recording device has a command register storing a command in accordance with said setting sequence;

an authentication processing command sequence for executing authentication processing between said external apparatus and said recording device, and an encryption processing command sequence for executing encryption processing relating to transferred data between said external apparatus and said recording device; and

a sequence is set such that a command identifier corresponding to said authentication processing command sequence

is executed in a step before a command sequence corresponding to said encryption processing command sequence.

41. The recording device according to Claim 40, characterized in that said encryption processing command sequence includes at least one of a command sequence including encryption key exchange processing for encryption data that is transferred from said external apparatus to said recording device and stored in storing means in said recording device, or a command sequence including an encryption key exchange processing for encryption data that is stored in the storing means in said recording device and transferred from said storing device to said external apparatus.

42. The recording device according to Claim 40, characterized in that said control section set an authentication flag indicating that authentication is done if authentication is established by the authentication processing of said external apparatus and said recording device, and executes command management control that enables execution of said encryption processing command sequence during the authentication flag is set, and said control section resets said authentication flag in executing said authentication processing command sequence anew.

15. The recording device according to Claim 43, characterized in that said data processing system has a configuration in which said

control section manages an order of command execution based on said setting sequence and said command identifier in said encryption key exchange processing, and said control section does not accept command processing that is different from said setting sequence from an external apparatus including said external apparatus during a series of command execution relating to said key exchange processing.

44. The recording device according to Claim 38, characterized by having a configuration in which:

said recording device has a key block storing an authentication key applied to authentication processing between said external apparatus and said recording device and a storing key as an encryption key of data stored in a data storage section in said recording device; and

said control section in an encryption processing section of said recording device receives a command identifier from said external apparatus and executes authentication processing using the authentication key stored in said key block in accordance with said setting sequence, and executes encryption processing of data accompanying key exchange processing using said storing key after completing the authentication processing.

45. The recording device according to Claim 44, characterized by having a configuration in which:

said key block is composed of a plurality of key blocks storing an authentication key and a storing key that are different each other; and

said external apparatus notifies said recording device of one key block used in authentication processing and encryption processing of data as a designated key block out of said plurality of key blocks, and said recording device executes authentication processing using the authentication key stored in the designated key block and encryption processing of data using the storing key.

46. A data processing method in a data processing system comprising a first apparatus and a second apparatus for executing transmission of encryption data to each other, characterized in that said second apparatus executes command processing controlling steps for receiving a command identifier transferred from said first apparatus in accordance with a setting sequence defined in advance, taking out a command corresponding to the received command identifier from a register, and having the command executed, and in said command processing control, if the command identifier transferred from the first apparatus is a command identifier different from the setting sequence, processing of command corresponding to the command identifier is cancelled.

47. The data processing method according to Claim 46, characterized in that:

in said command processing controlling step, the setting sequence relating to the command identifier received from the first apparatus is a command number setting sequence in which numbers are sequentially incremented; and

said command processing controlling steps comprises:

a step of storing a receiving value of a received command number from said first apparatus in a memory; and

a determining step for determining coincidence of a new command number received from said first apparatus with the setting sequence based on the received command number stored in said memory and, if it is determined that the new received command number is different from the setting sequence in said determining step, executing resetting of the command number stored in said memory without performing command processing corresponding to the new received command number.

48. The data processing method according to Claim 46, characterized in that:

in said data processing method, said command processing controlling step is a step for executing:

an authentication processing command sequence for executing authentication processing between said first apparatus and said second apparatus; and

an encryption processing command sequence for executing encryption processing relating to transferred data between said first apparatus and said second apparatus; and

said setting sequence is a sequence for executing said authentication processing command sequence prior to said encryption processing command sequence.

49. The data processing method according to Claim 48, characterized in that said encryption processing command sequence includes at least one of a command sequence including encryption key exchange processing for encryption data that is transferred from said first apparatus to said second apparatus and stored in storing means in said second apparatus, or a command sequence including an encryption key exchange processing for encryption data that is stored in the storing means in said second apparatus and transferred from said second apparatus to said first apparatus.

50. The data processing method according to Claim 48, characterized by comprising, in said data processing method, an authentication flag setting step of setting an authentication flag indicating that authentication is done if authentication is established by the authentication processing of said first apparatus and said second apparatus, and characterized in that said command processing controlling step executes command

management control that enables execution of said encryption processing command sequence during the authentication flag is set.

51. The data processing method according to Claim 50, characterized by comprising the step of resetting, in said data processing method, said authentication flag in executing said authentication processing command sequence anew.

52. The data processing method according to Claim 49, characterized by comprising, in said command processing controlling step in said data processing method, managing an order of command execution based on said setting sequence and said command identifier during execution of a series of commands relating to said key exchange processing, and not accepting command processing that is different from said setting sequence from an external apparatus including said first apparatus.

53. A program providing medium for providing a computer program for causing a computer system to execute data processing in a data processing system that comprises a first apparatus and a second apparatus for executing transmission of encryption data to each other, characterized by comprising:

a command processing controlling step of receiving a command identifier transferred from said first apparatus to said second apparatus in accordance with a setting sequence defined in advance,

executes only a command number that complies with the sequence defined in advance. Since a command sequence is set to execute an authentication processing command prior to an encryption processing command, only the recorder/reproducer that has completed the authentication processing can execute storing in the recording device and reproduction processing of contents, and contents utilization by an illegal instrument that has not completed the authentication processing can be eliminated.